IN THE CLAIMS:

Claims 1 to 105 (cancelled)

106. (currently amended) A method of protecting from theft and misuse bankcard data from merchant computer systems and securely selecting any one of a plurality of bankcards of a customer at a merchant point of sale interface for a payment transaction to a merchant comprising the steps of:

a. enabling selecting a debit card transaction requiring entry of a PIN in a merchant point of sale (POS) interface, enabling entering of (i) a customer identifier, without customer identity data, by a payment card that encodes the customer identifier and (ii) a bankcard specific personal identification number (CPIN) in the merchant point of sale (POS) interface;

b. enabling sending the customer identifier and the CPIN to an adapted prior art merchant gateway, along with the payment transaction data that includes a merchant identifier and a payment amount;

c. interfacing by the adapted prior art merchant gateway with a payment card system, and sending to the payment card system the customer identifier and the CPIN;

d. having stored customer bankcard data in the payment card system, wherein, each bankcard is identified with a separate CPIN, identifying a particular bankcard data of the customer and verifying the customer by the bankcard specific CPIN in the payment card system;

e. returning to the adapted prior art merchant gateway the bankcard data corresponding to the customer identifier and the CPIN from the payment card system;

f. assembling by the adapted prior art merchant gateway, a payment transaction record to include the bankcard data from the payment card system and the payment transaction data, and by submitting [[a]] the payment transaction record to a bankcard authorization network, wherein the method does not transfer bankcard identity data to the merchant computer systems [[~~POS interface~~]].

107. (currently amended) The method as in claim 106, comprising further steps of:

encoding [[~~encrypting a~~]] the customer identifier [[~~to be the customer identifier~~]] without customer identity data on the payment card with an algorithm and decoding [[~~decrypting~~]] the customer identifier with the algorithm in the payment card system to get [[~~identify~~]] the customer identifier.

108. (previously presented) The method as in claim 106, comprising further steps of:

a. delivering the payment card to the customer;

b. enabling entering the bankcard data and self-selecting a CPIN for each of the bankcards of the customer in the payment card system.

109. (currently amended) A [[~~payment card that operates with a~~]] payment card system and that protects private data of a customer from theft and misuse from merchant computer systems in customer to merchant payment transactions, comprising:

a. a payment card with a substrate;

b. a customer identifier that is without customer identity data, the customer identifier maps to the payment card system;

c. the customer identifier is encoded to be an encoded customer identifier when the customer identifier is encoded with an algorithm in the payment card system and then embeds a reference code that references the algorithm;

d. the substrate encoded with the encoded customer identifier and the substrate printed with an alias name selected by the customer.

110. (currently amended) The payment card system as in claim 109, comprising:
the encoding medium is a magnetic strip.

111. (currently amended) The payment card system as in claim 109, comprising:

the customer-identifier is self-created by the customer.

112. (currently amended) The payment card system as in claim 109, further comprising:

a. the encoded customer identifier from the payment card used for a payment transaction at a merchant point of sale (POS), along with entry of a bankcard specific personal identification number (CPIN) by the customer are routed from the POS to an adapted prior art merchant gateway, the adaptation in the prior art merchant gateway routes the encoded customer identifier and the CPIN to the payment card system;

b. the payment card system decodes the encoded customer identifier using the algorithm that is referenced by the code present in the encoded customer identifier, the payment card system then maps the customer identifier and the CPIN to retrieve a specific bankcard data and returns the specific bankcard data to the adapted prior art merchant gateway.

113. (currently amended) The payment card system as in claim 112, further comprising:

the adapted prior art merchant gateway, after receiving the specific bankcard data from the payment system, assembles a payment transaction record using the specific bankcard data for submission of the payment transaction record to a bankcard authorization network, thereby the payment card operating with the payment card system does not transfer customer identity data to the merchant computer systems [[~~POS~~]].

114. (currently amended) A method of conducting a payment transaction that protects the privacy of customer identity and bankcard data, from theft and misuse from merchant computer systems, comprising the steps of:

a. enabling creating a customer identifier that is without customer identity data, the customer identifier maps to a payment card system;

b. encoding the customer identifier with an algorithm, and then embedding a reference code that references the algorithm in the payment card system, thus getting an encoded customer identifier;

c. delivering to a customer, a payment card with a substrate printed with an alias name selected by the customer and encoded with the encoded customer identifier.

115. (previously presented) The method as in claim 114, further comprising the steps of:

a. enabling using the payment card for the payment transaction at a merchant point of sale (POS) and entering a bankcard specific personal identification number (CPIN) by the customer;

b. enabling the POS routing a payment transaction record to an adapted prior art merchant gateway;

c. enabling identifying the use of the payment card at the POS, by the adapted prior art merchant gateway, and routing the encoded customer identifier and the CPIN of the payment transaction to the payment card system.

116. (previously presented)The method as in claim 115, further comprising the steps of:

decoding the encoded customer identifier by the payment card system using the algorithm that is referenced by the code in the encoded customer identifier, and using the customer identifier and the CPIN, retrieving specific bankcard data in the payment card system, and returning to the adapted prior art merchant gateway.

117. (currently amended) The method as in claim 116, further comprising the steps of:

enabling the adapted prior art merchant gateway, after receiving the specific bankcard data from the adapted prior art merchant gateway, to assemble a payment transaction record with the specific bankcard data for submitting the payment transaction record to a bankcard authorization network, wherein the payment card does not transfer customer identity data to the merchant computer systems [[~~POS~~]].

118. (previously presented) The method as in claim 114, further comprising the steps of:

a. enabling using the payment card for the payment transaction at a merchant point of sale (POS) and enabling entering a bankcard specific personal identification number (CPIN) by the customer;

b. connecting wirelessly by the merchant POS to the payment card system for routing a payment transaction record that includes a payment amount, a merchant identifier, a reference number, the encoded customer identifier, and the CPIN.

119. (previously presented) The method as in claim 118, further comprising the steps of:

receiving wirelessly the payment transaction record by the payment card system.

120. (previously presented) The method as in claim 119, further comprising the steps of:

decoding the encoded customer identifier by the payment card system using the algorithm that is referenced by the code in the encoded customer identifier, and using the customer identifier and the CPIN, retrieving specific bankcard data in the payment card system.

121. (currently amended) The method as in claim 120, further comprising the steps of:

assembling a payment transaction record with the specific bankcard data, the payment transaction record includes, a customer name, a bankcard number, an expiration date, the merchant identifier, the payment amount, and the reference number, and submitting the payment transaction record to a card authorization network via an adapted prior art merchant gateway.

122. (currently amended) The method as in claim 121, further comprising the steps of:

receiving a payment approval record by the payment card system from the card authorization network via the adapted prior art merchant gateway, the payment approval record [[~~that~~]] includes the reference number, the payment amount and a payment authorization number, and forwarding wirelessly the payment approval record to the merchant POS, wherein the payment card does not transfer customer identity and bankcard data to the merchant computer systems [[~~POS~~]].

123. (currently amended) A payment security system that provides identity security in use of bankcards, from merchant computer systems, comprising:

a. a customer identifier that is without customer identity data;

b. the customer identifier maps to a plurality of bankcard data of the customer, each bankcard data identified with a card specific personal identification number (CPIN) in the payment security system;

c. the customer identifier is encoded to be an encoded customer identifier when encoded with an algorithm from a list of such algorithms in a database maintained by the payment security system and then embeds a reference code that references the algorithm, the encoded customer identifier is then encoded on a payment card encoding mechanism, wherein the payment card and the CPIN is used by the customer at a merchant point of sale (POS) of a merchant system for conducting a payment transaction.

124. (currently amended) The payment security system as in claim 123, further comprising:

on swiping of the payment card and entry of the CPIN, the payment security system receives from the merchant POS, the encoded customer identifier and the CPIN, decodes the encoded customer identifier, using the customer identifier and the CPIN selects the specific bankcard data of the customer for processing the payment transaction with a bankcard processing network, wherein, the security system does not transfer the customer identity and customer bankcard data to the merchant computer systems.